DATA PROTECTION IMPACT ASSESSMENT (DPIA)

OVERVIEW

This procedure provides the guidance and documentation for the completion of a Data Protection Impact Assessment (DPIA) for any programme or project being undertaken within Plymouth City Council.

The procedure consists of two parts, the first part being a set of screening questions that will determine if the next part, the system assessment has to be completed.

All projects must undertake the screening questions and return the answers to the Information Governance Manager (IGM) so that due process can be shown to have been completed.

DATA PROTECTION IMPACT ASSESSMENT

Service overview	
Service Name	**EARLY HELP & TARGETED SUPPORT PROJECT**
Purpose of service	
To provide an Early Help & Targeted Support offer to families with CYP aged 0-19 aligned to the health localities. This will be delivered through co-location of multi-disciplinary staff to prevent escalation to specialist services and achieve positive outcomes for families.	
Overview of how the service operates	
Early Help - In order to deliver an effective integrated Early Help offer we will create a network of community-based Family Hubs, offering support to CYP aged 0-19, their families and carers. The Family Hub model is a 'one-stop-shop' for families with children of all ages, offering support and signposting. The locations of Family Hubs would need to align with local need and the most effective children's centre buildings, whilst recognising the interdependencies with the aims of the wellbeing hubs. **Targeted Support** - The project will create a small number of Targeted Support Teams; located so that they work across the PCC city-wide footprint. Co-location of practitioners working with more complex families would allow professionals to work creatively together, including shared assessments of need and risk, to ensure that any service offer is collectively managed and sequenced by a multi-disciplinary approach. Professionals will be deployed from the Targeted Support Teams to support Family Hubs staff and deliver interventions to families in the community, including the homes of CYP & families and from the family hubs themselves. The Targeted Support Teams would offer services such as crisis response to prevent escalation, as well as an interface with related services such as the parent and child offer and complex lives alliance. The EH&TS project has adopted a system approach to strategic participation, to ensure the voices of children, young people & families (CYP&F) are captured and embedded into system improvements.	

Information assessment	**YES/NO**
Does the service process information about individuals?	**Y**
Will the project compel individuals to provide information about themselves?	**Y**

Will information about individuals be disclosed to organisations or people who have not previously had routine access to the information?	**Y**
Are you using information about individuals for a new purpose or in a new way that is different from any existing use?	**Y**
Does the project involve you using new technology which might be perceived as being privacy intrusive? For example, the use of biometrics, facial recognition or location tracking.	**N**
Is the information to be used about individuals' health and/or social wellbeing?	**Y**
Does the information contain any financial details? Including individuals or businesses	**Y**
Will the project result in personal information being aggregated?	**Y**

Information flows The collection, use and deletion of personal data should be described here and it may also be useful to refer to a flow diagram or another way of explaining data flows.	
Type of personal data being used :	As required by **Early Help Assessment Tool.**
Data origin	Clients: Family members; other agencies (signatories to ISA); existing systems (e.g. Capita ONE; CareFirst; SystmOne etc.)
Data is shared with?	PCC staff; Police; Private Sector (dependant of provider);Third Sector; Health professionals
Brief Description of the flow of data/information	Consensual information and data will be gathered from individuals, their families & professionals as required to achieve outcomes. Information & Data will be shared & stored in accordance with Information Sharing Agreement

Legal Requirements	
Are there any legal enablers or legislation, of which you are aware, that aid in the use of personal information for the purposes you have specified in this questionnaire? If so, please specify in Further Information (below).	

Further information – Please provide any further information that will help in determining the Data Protection impact.

- Data Protection Act 2018 http://www.legislation.gov.uk/ukpga/2018/12/contents/enacted
- Information Sharing Agreements with partners
- All employees and agents of the Council who processes Personal Data about living individuals must comply with the eight Data Protection Principles
- When considering this DPIA it is important to have due regard to the public sector equalities duties imposed upon the Council by section 149 Equalities Act 2010
- Commissioning contracts may contain additional data protection requirements in the T&Cs-

DPIA outcome Does the system require further assessment for compliance?	
System assessment needed:	Yes

Risks (Privacy / Availability / Integrity)

List any identified risks to privacy and personal information of which the project is currently aware. Risks to be populated in the Risk Register.

	Risk Description **(to individuals, to the Authority or to wider compliance)**	**Proposed Risk solution (Mitigation)**	**Is the risk reduced, transferred, or accepted? Please specify / justify.**
1	Unauthorised person accesses Council data via system	• Access to data is restricted by Council active directory groups. Only authorised staff are placed in the groups. • Auditing of access, view and input can be monitored using current activity/auditing procedure • The system is regularly PEN tested when any updates and new functionality are released. The Capita ONE system is fully supported by DELT. • System is monitored for security breaches and unusual activity by the provider and appropriate action escalated through DELT as required.	Reduced
2	Inappropriate handling or use of client data	• Established legislation, regulation, policy & procedures, together with Staff training and Information Sharing Agreements between partners • Procurement QA and contractual T&Cs relating data transfer between providers	Reduced
3	Individual staff data (pay & grading) may be released to other staff/management	• S: Drive storage locked down to authorised persons only. • Sanitise structural data. Remove individual names for positions within staffing structure diagrams, before inclusion in consultation documents and briefings	Reduced

		• Stakeholders involved in the procurement will sign declaration of interest and confidentiality agreements	
4	Data transferred to system is intercepted, accessed and / or changed by unauthorised people	• The File Uploader function of the Capita ONE Professional Portal has been upgraded by the provider to give additional validation checks. This includes invoking a virus checker to verify the contents of the file being uploaded and to detect potentially malicious / disruptive content.	Reduced
5	Authorised people retain Council data accessed / transferred via system longer than necessary	• Deletion in accordance with retention schedule. Information is created as an information asset for any ongoing assessment and identification of need, in order to provide the necessary support.	Reduced
6	Client data is retained by system supplier longer than necessary	• System suppliers do not have access to the data	Accepted
7	System data is merged with data from other organisations	• Data is merged with data from other organisations, as this is the purpose of the programme • Procurement QA and contractual T&Cs relating data transfer between providers	Accepted
8	System data is stored in a location that is not compatible with the data protection Act	• Data is stored in the UK	Accepted
9	Council data is copied and archived by unauthorised third parties	• Third parties do not have access to the data in order to archive	Accepted
10	System is used by employees for purposes other than the stated purpose	• The Capita ONE Professional Portal operates on a secure web portal with two-factor authentication for users. The Gateway Administration team verify and authorise users, which controls the data and information they are able to see. • The File Uploader function of the Capita ONE Professional Portal has been upgraded by the provider to give additional validation checks.	Reduced
11	Data subject access rights cannot be enforced by system	• Data and information collected will be subject to the requirements of the DPA 2018 and PCC information protocols, policy & procedures. We	Accepted

		have an information and communications technology strategy and an information management strategy that provides a framework for making best use of our information so that decision making, reporting and communications are based on accurate, available and trusted knowledge resources.	
12	Data subject deletion rights cannot be enforced by system	• The Capita system has the ability to delete individual records via the Archive and Delete function. This is strictly controlled by business system administrators.	Reduced
13	Data subject correction rights cannot be enforced by system	• Business System Administrators have the ability to correct data at database level where appropriate.	Reduced
14	System is taken offline maliciously, resulting in service not being delivered to clients.	• System is hosted internally and monitored by a security specialist company • Business continuity process exit for the service	Accepted
15	Malicious person registers on system to access data	• System access is controlled internally, with a formal approval process.	Accepted
16	System is compromised and used to deliver malicious software to Council infrastructure	• A full ITHC is conducted annually to ensure no vulnerabilities can be exploited.	Accepted
17	Components of system installed on Council infrastructure used to compromise the infrastructure	• No Components are installed	Accepted
18	System allows malicious software to be transferred from 3rd party network to Council infrastructure	• All communication with third parties is scanned and verified by the Council's perimeter security	Accepted

Final assessment Please refer to separate assessment documentation.			
System assessment reference:	**PEOP-000010**		
System addresses identified risks:	**Yes**		
System is DPA compliant:	**Yes**		
System is fit for purpose:	**Yes**		
Sign off name	**Sign off role**	**Date**	**Signature**

John Finch	PCC IGM	9th May 2019